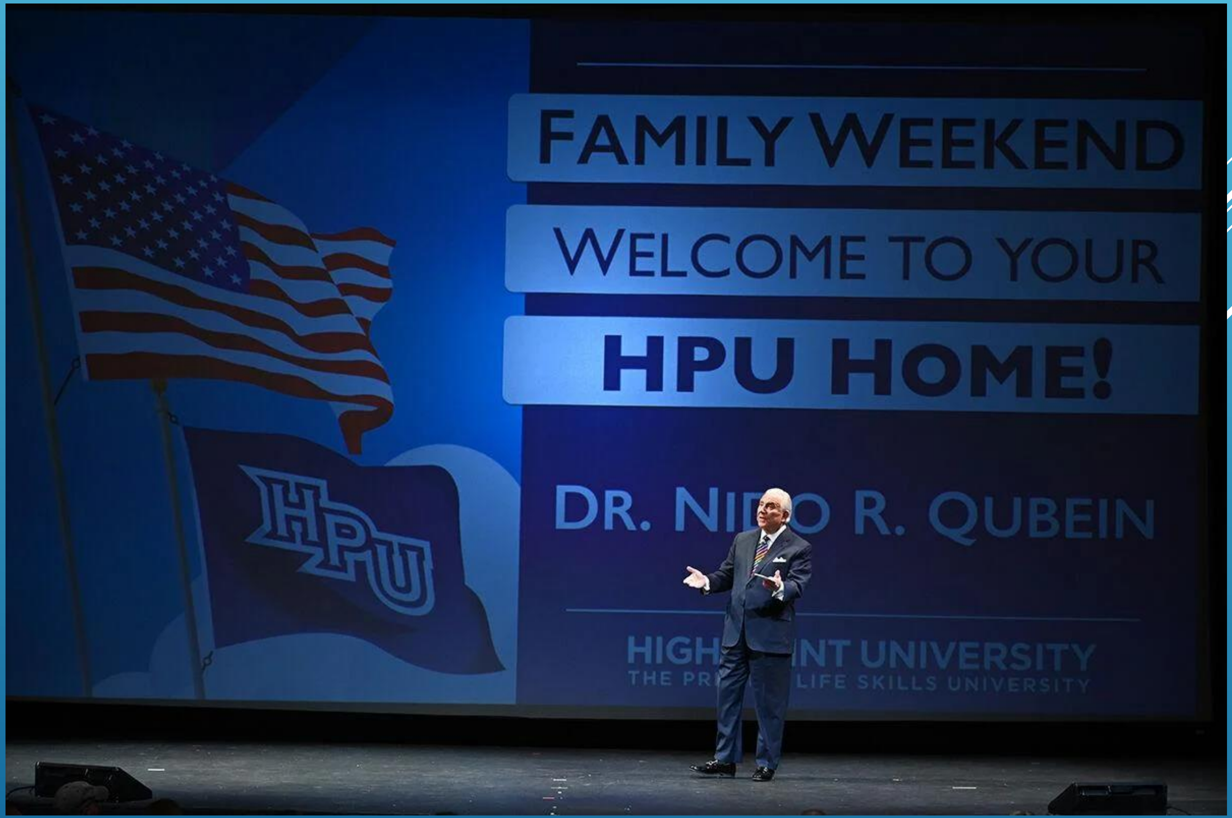
GMIS
NEW JERSEY
An Association Of Government IT Leaders

Ransomware

A firsthand account

Your worst nightmare

Lessons Learned and a new approach!

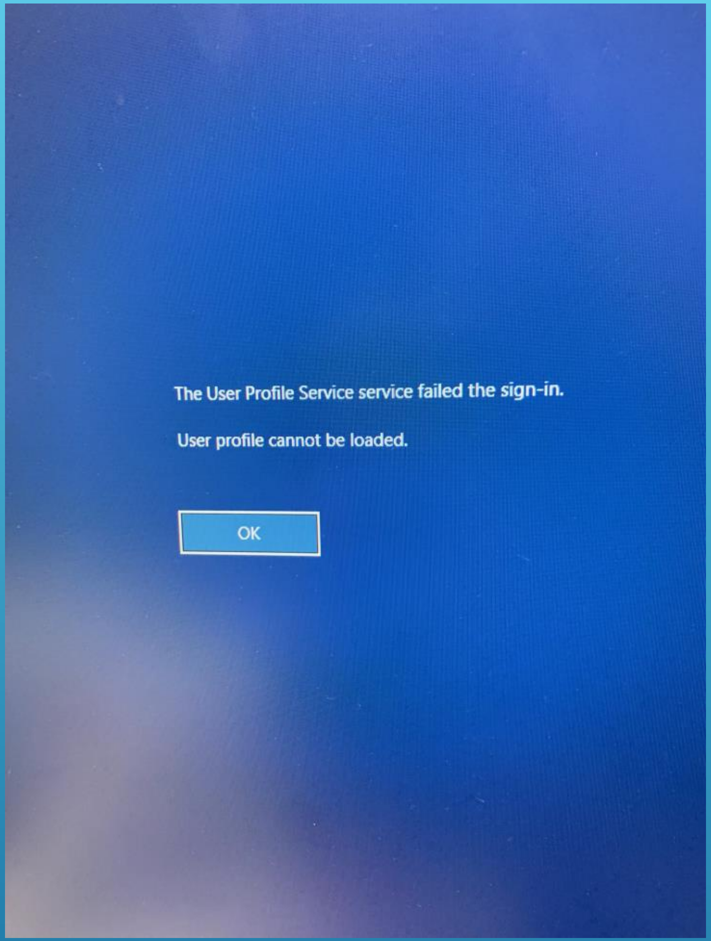


The Day started out with lots of hope!

But then the whole world came crashing in….

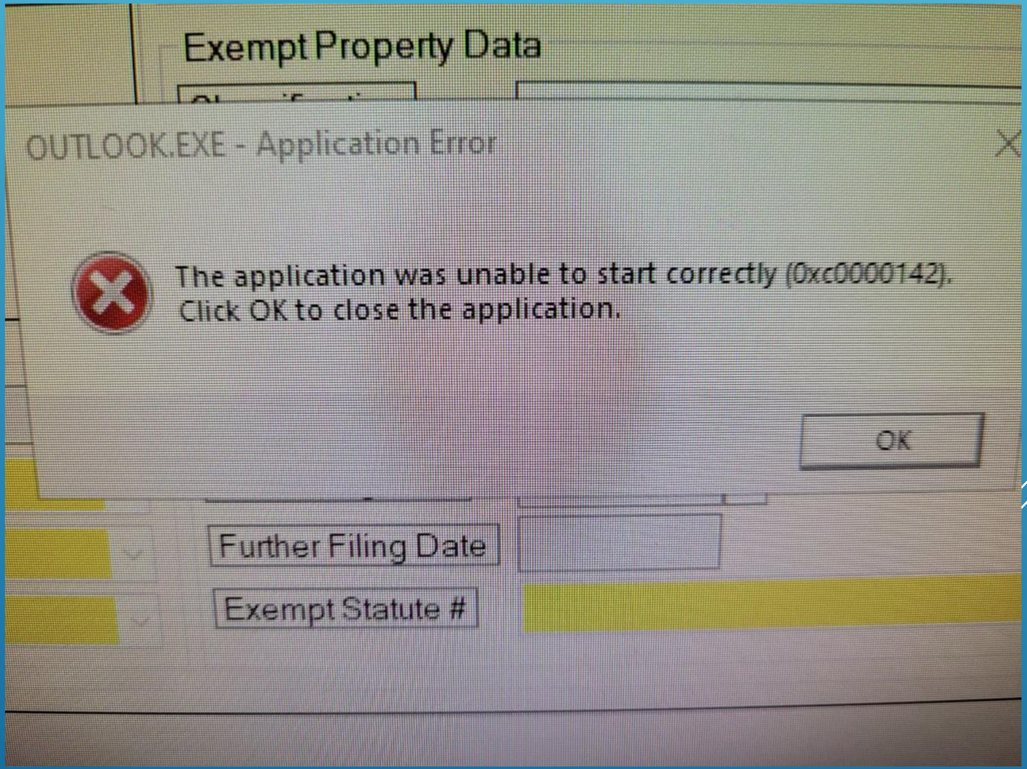
The call no IT person wants to get….

GMIS
NEW JERSEY
An Association Of Government IT Leaders



The User Profile Service service failed the sign-in.

User profile cannot be loaded.



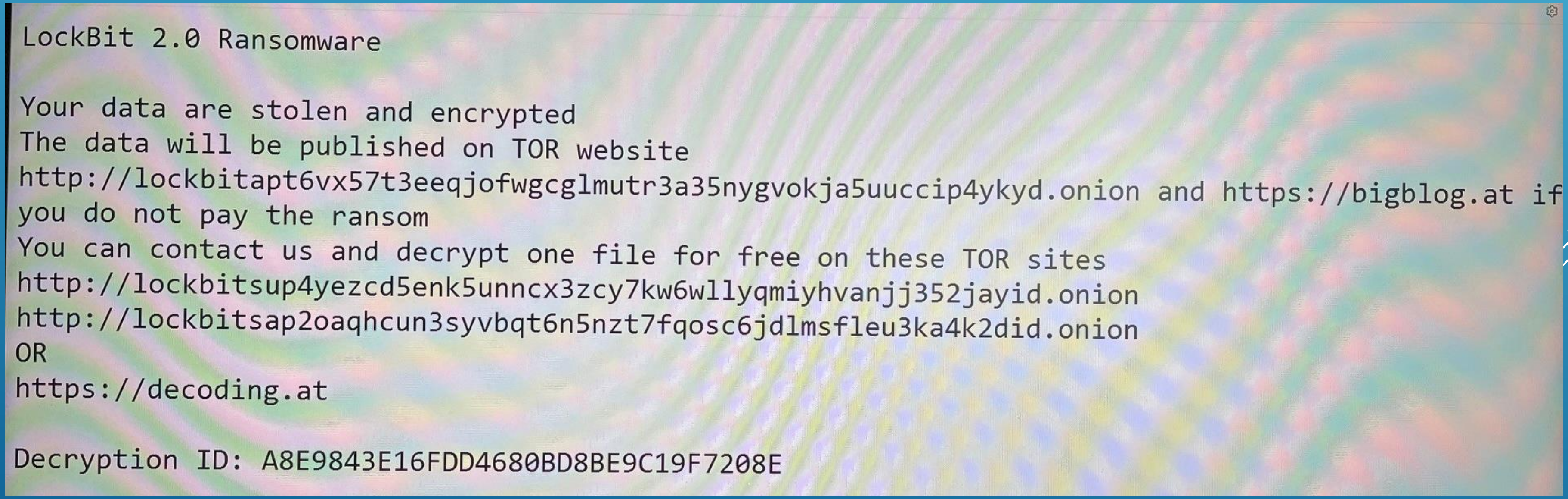
Exempt Property Data

OUTLOOK.EXE - Application Error

The application was unable to start correctly (0xc0000142). Click OK to close the application.

7:45 to 8:00 am
Users Unable to either logon to computer or access programs.
More to come!!!

- First steps
  - As a one man shop, troubleshoot remotely
- Have Users reboot computers
  - Not thinking a breach but a network issue.
- Contact consultant
  - If you have a limited staff, a consultant to assist is a must!
  - If you have no staff, then all departments need to have your consultants contact info.
- Consultant remotely logs into servers
  - Worst fear is confirmed!!
  - Ransomware Attack!

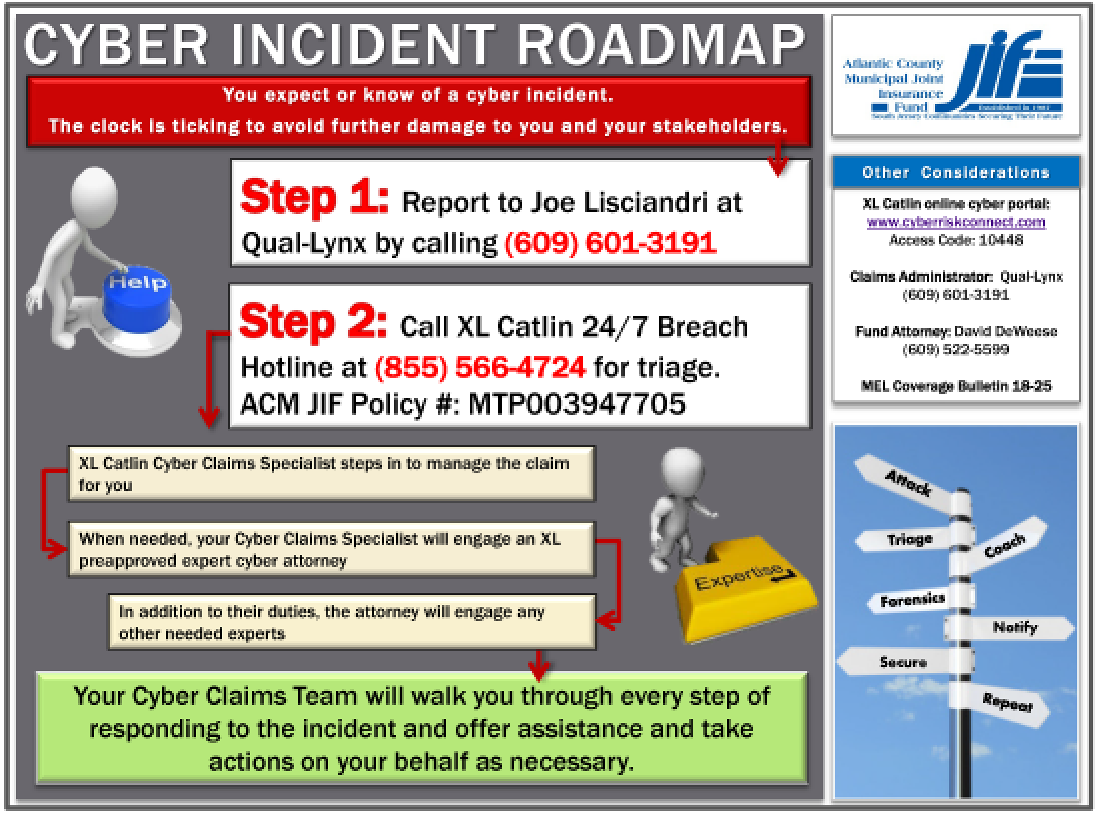


```
LockBit 2.0 Ransomware

Your data are stolen and encrypted
The data will be published on TOR website
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion and https://bigblog.at if
you do not pay the ransom
You can contact us and decrypt one file for free on these TOR sites
http://lockbitsup4yezcd5enk5unncx3zcy7kw6wllyqmiyhvanjj352jayid.onion
http://lockbitsap2oaqhcun3syvbqt6n5nzt7fqosc6jdlmsfleu3ka4k2did.onion
OR
https://decoding.at

Decryption ID: A8E9843E16FDD4680BD8BE9C19F7208E
```

- Immediate Steps!
- Protect the network
  - All Servers removed from Network and Internet Access
    - All Network cards disabled
    - If you are running virtual machines this can be done remotely, otherwise you must physically unplug the network cards.
  - ALL workstations MUST be physically shut down and network cables unplugged.
    - Machines MAY NOT be turned back on.
    - You must find ALL devices that are connected
    - All remote sites must be reviewed.
  - IF Police or other remote networks have physical connections they must be disconnected.
  - The entire network must be isolated!

GMIS NEW JERSEY
An Association Of Government IT Leaders

Follow your Cyber Incident Roadmap



CYBER INCIDENT ROADMAP

You expect or know of a cyber incident.
The clock is ticking to avoid further damage to you and your stakeholders.

Atlantic County Municipal Joint Insurance Fund JIF

Step 1: Report to Joe Lisciandri at Qual-Lynx by calling (609) 601-3191

Step 2: Call XL Catlin 24/7 Breach Hotline at (855) 566-4724 for triage. ACM JIF Policy #: MTP003947705

XL Catlin Cyber Claims Specialist steps in to manage the claim for you

When needed, your Cyber Claims Specialist will engage an XL preapproved expert cyber attorney

In addition to their duties, the attorney will engage any other needed experts

Your Cyber Claims Team will walk you through every step of responding to the incident and offer assistance and take actions on your behalf as necessary.

Other Considerations

XL Catlin online cyber portal:
www.cyberriskconnect.com
Access Code: 10448

Claims Administrator: Qual-Lynx
(609) 601-3191

Fund Attorney: David DeWeese
(609) 522-5599

MEL Coverage Bulletin 18-25

GMIS
NEW JERSEY
An Association Of Government IT Leaders

VALUE ADDED SERVICE:

eRisk Hub

- Go to https://www.eriskhub.com/xl.php
- Complete Registration Form
- Once Registered you will have immediate access to the portal with User ID & password created during registration
- You will need to enter the ACM JIF's Access Code to complete your registration. If you do not have this code, please contact any of the JIF Administrative Team Members at RPA (a division of Gallagher): (https://acmjifmembers.org/wp/about/contact-us/)

The **eRisk Hub** is a private web-based portal containing information and technical resources that can assist you in the prevention of network, cyber and privacy losses and support you in the timely reporting and recovery of losses if an incident occurs. [br]The eRisk Hub portal is an internet-based service that features news, content and services from leading practitioners in risk management, computer forensics, forensic accounting, crisis communications, legal counsel, and other highly-specialized segments of cyber risk.

eRisk Hub is a free service to members of the ACM JIF.

Step 2. **IT IS IMPORTANT TO CALL THE BREACH HOTLINE NUMBER AT THE EARLIEST TIME POSSIBLE, IF A BREACH HAS BEEN SUSPECTED OR HAS OCCURED!**

By calling the XL Data Breach Hotline number, you will receive immediate triage assistance from the Law Firm of Lewis Brisbois Bisgaard & Smith. **XL Data Breach Hotline: 1-855-566-4724**

It is important call the breach hotline at the earliest time possible if a breach has been suspected. Calling the hotline will begin a process of investigation that will determine if a claim should be filed. Calling the hotline **does not** meet the requirement of notification of a claim under the policy conditions it does however reduce potential claims and the amount spent by getting out in front of any possible breach situation. If you wait until a demand for damages is received by one of the members it's far too late to take action to mitigate the fallout from a breach.

ALL DEPARTMENTS MUST HAVE A COPY

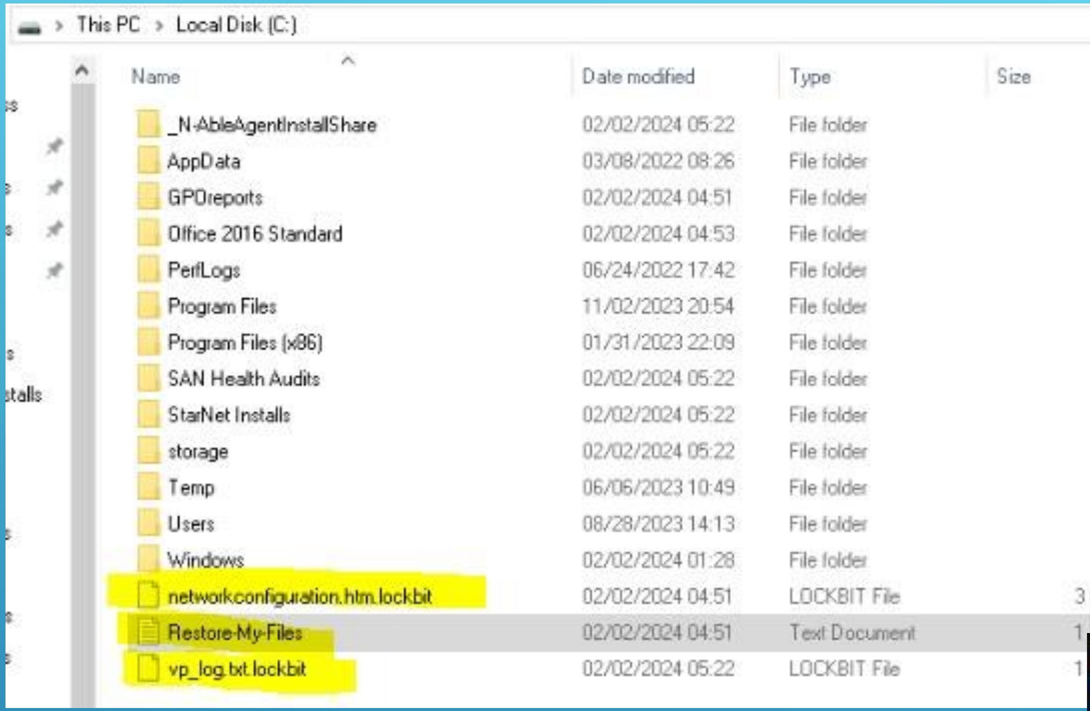
Day 1-4 – Analysis and Planning

- Determine extent of damage
  - Remove all servers from Network
  - Disconnect and turn off all workstations
    - Verify ALL locations accounted for!

- Since was a weekend no issues with connectivity!
  - Thankfully!
- Setup up meetings and calls with JIF attorneys
  - Spent all day on phone
  - GET ALL THE INFO YOU CAN!
    - WILL NEED TO REPEAT IT MANY MANY TIMES!
- Discussions with City Administration
  - Review extent of Damage
  - Discuss plan for remediation
- Review with consultant extent of damage
  - Discuss plan to begin repair
  - Servers
    - Begin server repair and rebuild
  - Workstations
    - Plan to rebuild

GMIS
NEW JERSEY
An Association Of Government IT Leaders

Kerberos Key was compromised
This caused all users to not be able to log onto their machines!



This PC › Local Disk (C:)

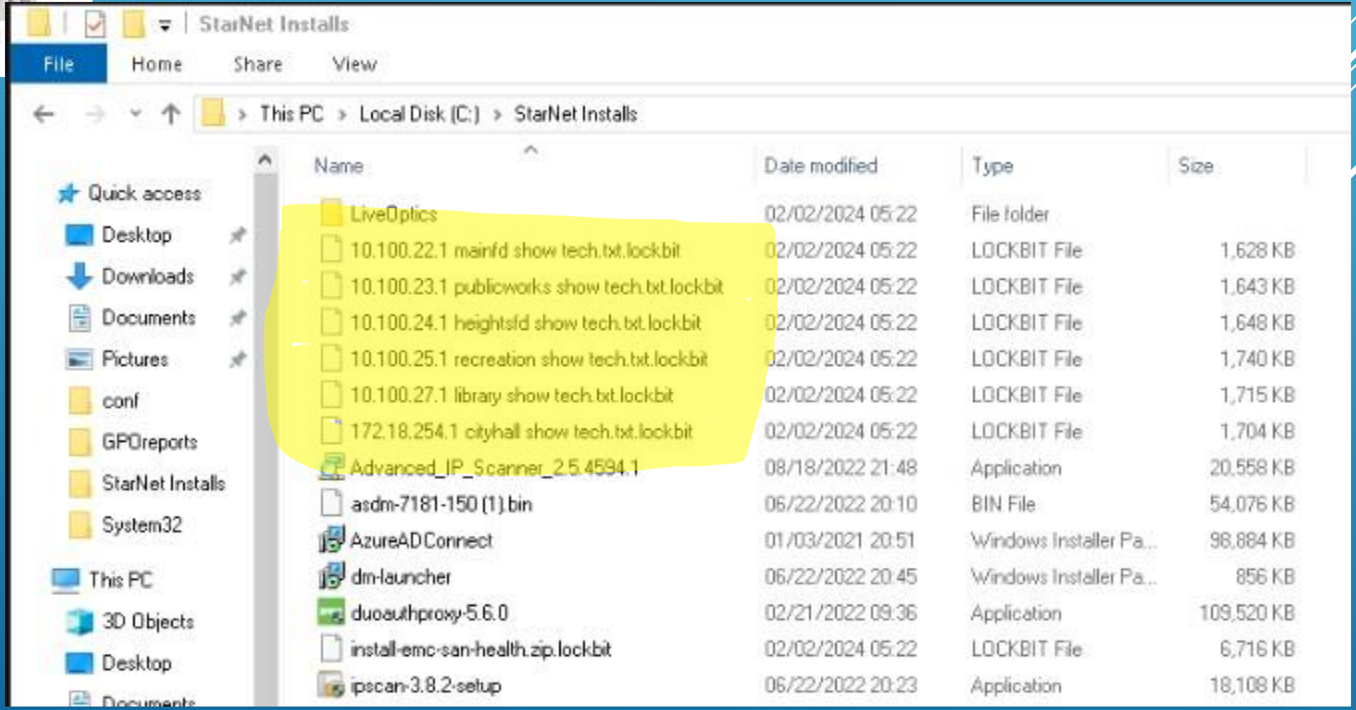
Name	Date modified	Type	Size
_N-AbleAgentInstallShare	02/02/2024 05:22	File folder	
AppData	03/08/2022 08:26	File folder	
GPOreports	02/02/2024 04:51	File folder	
Office 2016 Standard	02/02/2024 04:53	File folder	
PerfLogs	06/24/2022 17:42	File folder	
Program Files	11/02/2023 20:54	File folder	
Program Files (x86)	01/31/2023 22:09	File folder	
SAN Health Audits	02/02/2024 05:22	File folder	
StarNet Installs	02/02/2024 05:22	File folder	
storage	02/02/2024 05:22	File folder	
Temp	06/06/2023 10:49	File folder	
Users	08/28/2023 14:13	File folder	
Windows	02/02/2024 01:28	File folder	
networkconfiguration.htm.lockbit	02/02/2024 04:51	LOCKBIT File	3 KB
Restore-My-Files	02/02/2024 04:51	Text Document	1 KB
vp_log.txt.lockbit	02/02/2024 05:22	LOCKBIT File	1

GMIS

NEW JERSEY

An Association Of Government IT Leaders

All Servers and Workstations showed similar file platforms!



This PC › Local Disk (C:) › StarNet Installs

Name	Date modified	Type	Size
LiveOptics	02/02/2024 05:22	File folder	
10.100.22.1 mainfd show tech.txt.lockbit	02/02/2024 05:22	LOCKBIT File	1,628 KB
10.100.23.1 publicworks show tech.txt.lockbit	02/02/2024 05:22	LOCKBIT File	1,643 KB
10.100.24.1 heightsfd show tech.txt.lockbit	02/02/2024 05:22	LOCKBIT File	1,648 KB
10.100.25.1 recreation show tech.txt.lockbit	02/02/2024 05:22	LOCKBIT File	1,740 KB
10.100.27.1 library show tech.txt.lockbit	02/02/2024 05:22	LOCKBIT File	1,715 KB
172.18.254.1 cityhall show tech.txt.lockbit	02/02/2024 05:22	LOCKBIT File	1,704 KB
Advanced_IP_Scanner_2.5.4594.1	08/18/2022 21:48	Application	20,558 KB
asdm-7181-150 (1).bin	06/22/2022 20:10	BIN File	54,076 KB
AzureADConnect	01/03/2021 20:51	Windows Installer Pa...	98,884 KB
dm-launcher	06/22/2022 20:45	Windows Installer Pa...	856 KB
duoauthproxy-5.6.0	02/21/2022 09:36	Application	109,520 KB
install-emc-san-health.zip.lockbit	02/02/2024 05:22	LOCKBIT File	6,716 KB
ipscan-3.8.2-setup	06/22/2022 20:23	Application	18,108 KB

LockBit Statistics

Percentage of ransomware incidents attributed to LockBit:

- Australia: From April 1, 2022, to March 31, 2023, LockBit made up 18% of total reported Australian ransomware incidents. This figure includes all variants of LockBit ransomware, not solely LockBit 3.0.
- Canada: In 2022, LockBit was responsible for 22% of attributed ransomware incidents in Canada.[10]
- New Zealand: In 2022, CERT NZ received 15 reports of LockBit ransomware, representing 23% of 2022 ransomware reports.
- United States: In 2022, 16% of the State, Local, Tribal, and Tribunal (SLTT) government ransomware incidents reported to the MS-ISAC were identified as LockBit attacks. This included ransomware incidents impacting municipal governments, county governments, public higher education and K-12 schools, and emergency services (e.g., law enforcement).

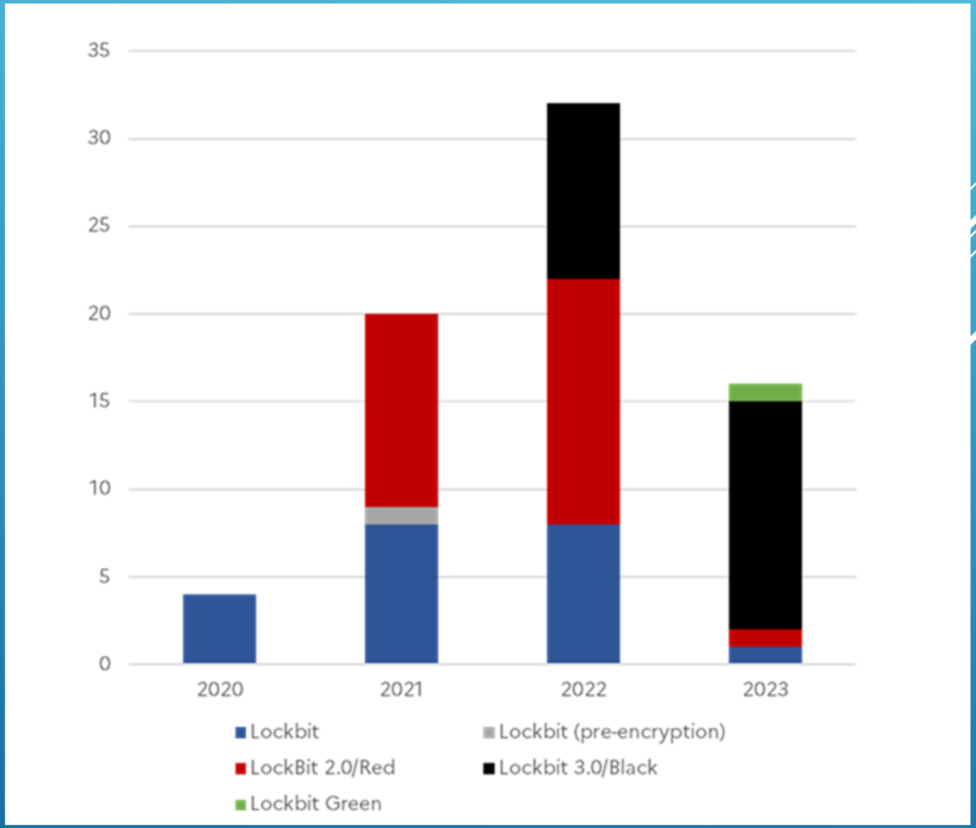
Number of LockBit ransomware attacks in the U.S. since 2020:

- About 1,700 attacks according to the FBI.

Total of U.S. ransoms paid to LockBit:

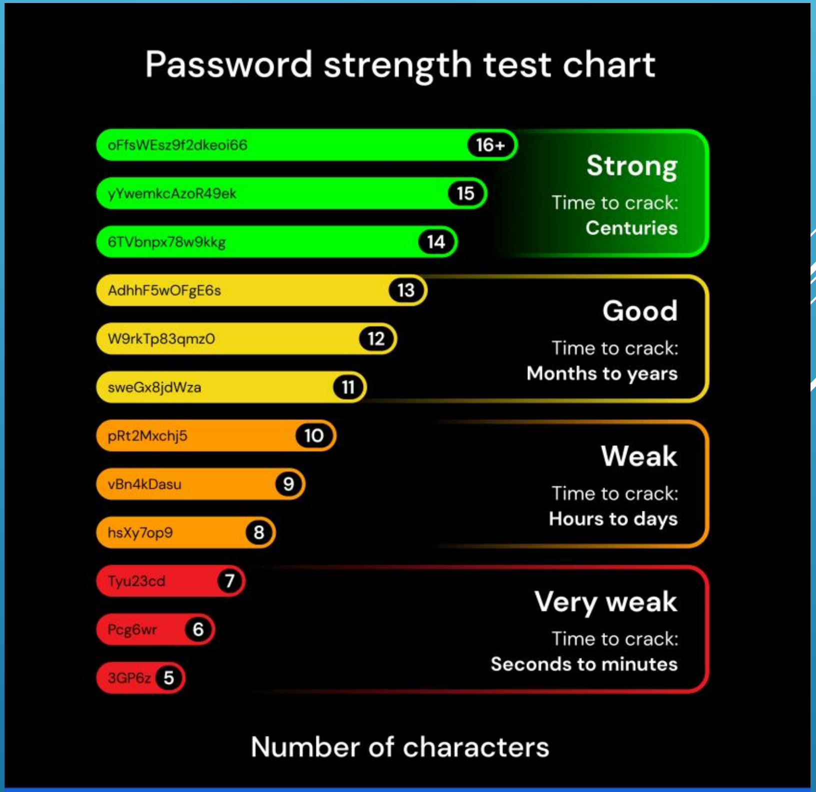
- Approximately $91M since LockBit activity was first observed in the U.S. on January 5, 2020.

GMIS
NEW JERSEY
An Association Of Government IT Leaders



Remediation Steps

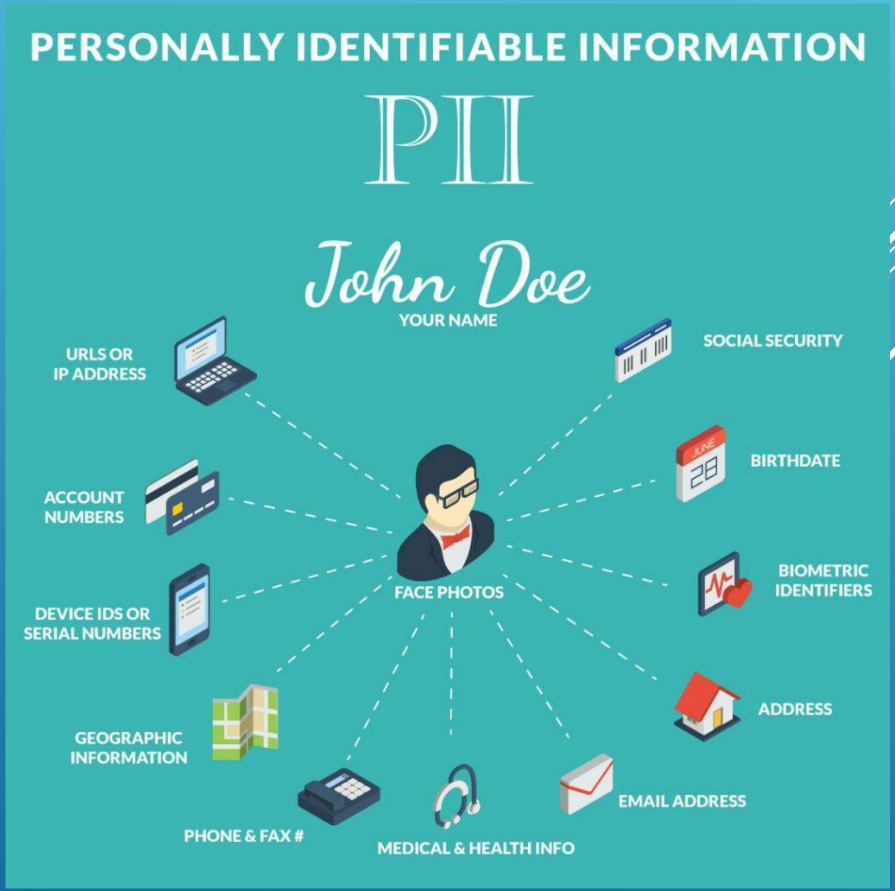
- Servers
  - Rebuild all servers from known good backups
    - Luckily only had to go a few days backs for clean BU
    - Unfortunately, remote sites had frozen and back several months.
      - Ensure BU reporting in place!
    - Back in service except remote in 5 days.
    - Ensure Domain Controllers clean and back 1st.
- Workstations
  - Rebuild or reimage all infected machines
  - IF have new machines put in place
    - Do not use old Hard drives if possible.
  - Ensure AV and all security programs put back in place.
  - Took about 4 weeks to complete.
- In Between time
  - Used Laptops to access Email and Cloud platforms
- User Profiles
  - All profiles rebuilt and cleaned.
  - Passwords reset a minimum of 3 times to ensure clean.
    - Ensure password reset policy in place!
    - Have Complexity policy in place.



JIF Remediation

- Forensic Auditor
  - Assigned by JIF and Attorney’s
  - Will assign forensic team to review breach
  - Contracts to be signed.
    - Get on these immediately
    - Do not wait to approve
    - Time is money!! And Time is critical in auditing!
  - Save logs immediately!
  - Will ask for drive data from servers and workstations
    - Will look at servers first!
    - Looking to determine who threat actor got in.
    - What they looked at when they got in.
  - Depending on what and how will depend on what you need to do.
    - PII info
    - Personal Data
  - JIF and Attorneys will advise next steps.
    - Do you need to notify the public??
    - It Depends!

GMIS
NEW JERSEY
An Association Of Government IT Leaders

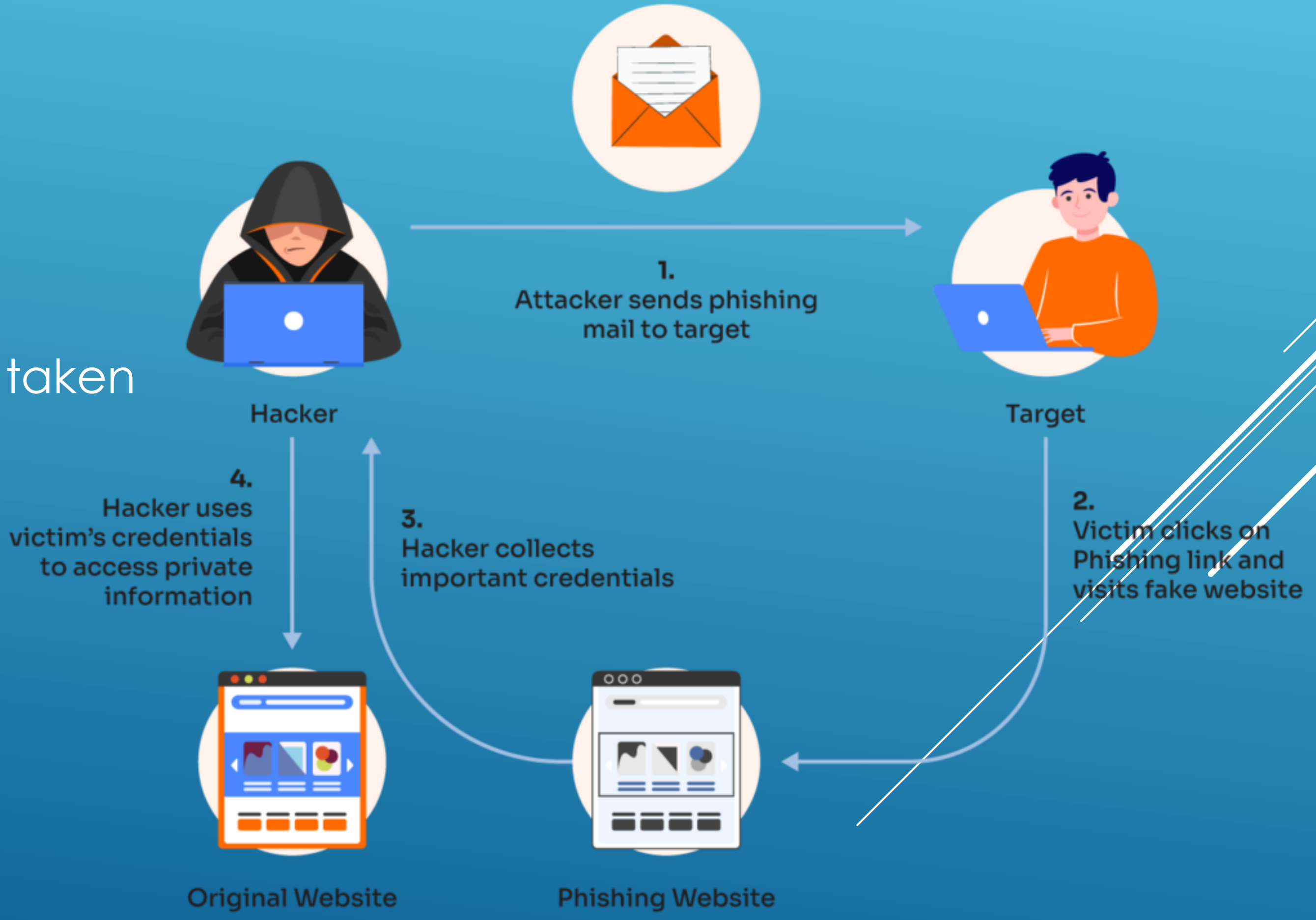


So, What Happened??

- Threat actor got in via the VPN.
- Was able to compromise someone's credentials
  - Because we did not have logs saved unable to determine who or when.
  - Critical to save logs - set up log server!
- Did not review or take any PII info!
  - Whew! Saved us!
  - Did not have to notify the public!
  - Threat Actor DID NOT contact us!
  - We DID NOT contact them!
- This is NOT the norm! We got lucky!
- Contact or payment is based on data taken
- Attorneys and forensics will advise

GMIS NEW JERSEY

An Association Of Government IT Leaders


Hacker
1. Attacker sends phishing mail to target
Target
2. Victim clicks on Phishing link and visits fake website
3. Hacker collects important credentials
4. Hacker uses victim's credentials to access private information
Original Website
Phishing Website

What we learned!

We are doing a lot right

It’s all in the details

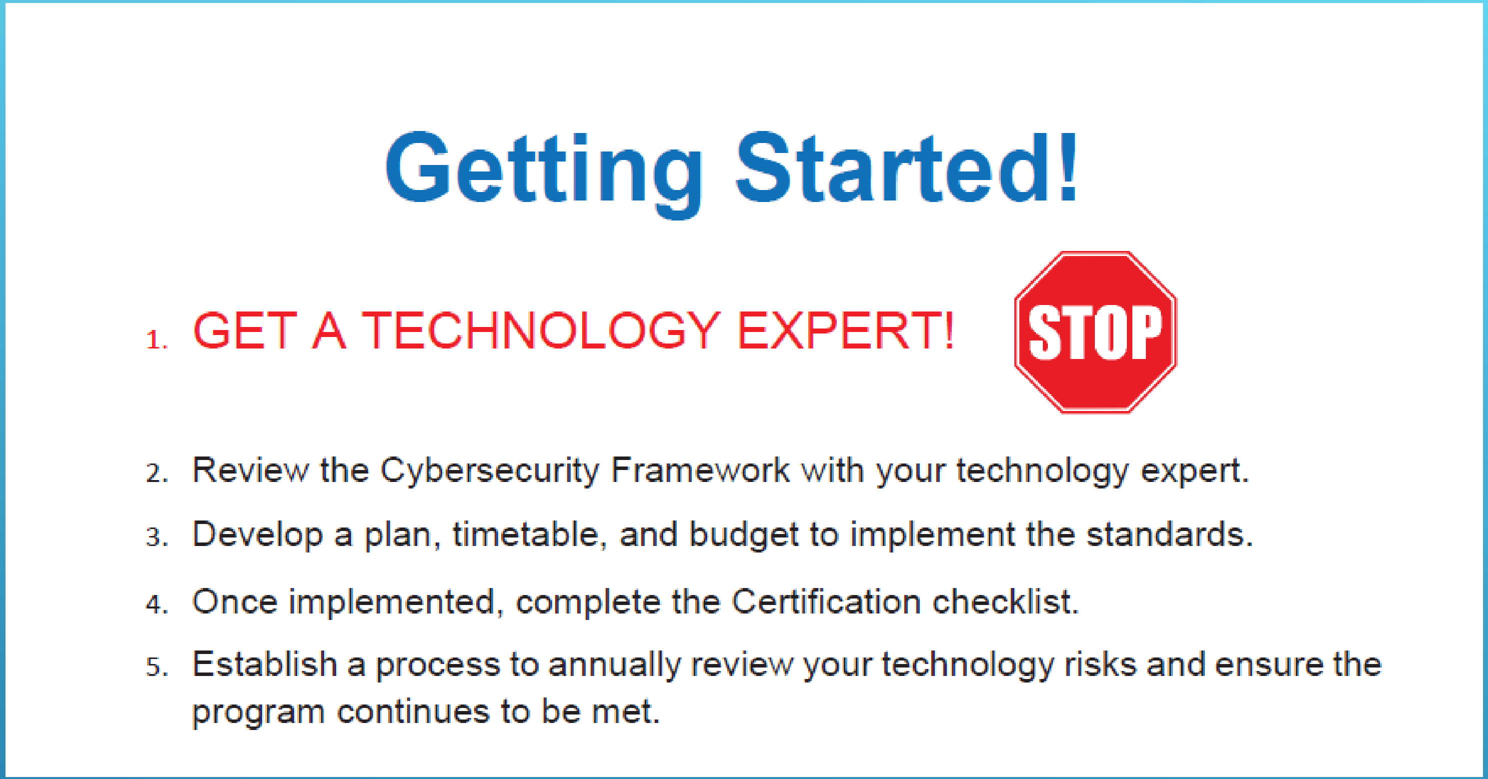
BUT….

There is a lot More to do!

And Yes, there is Time and money Involved!

GMIS NEW JERSEY

An Association Of Government IT Leaders



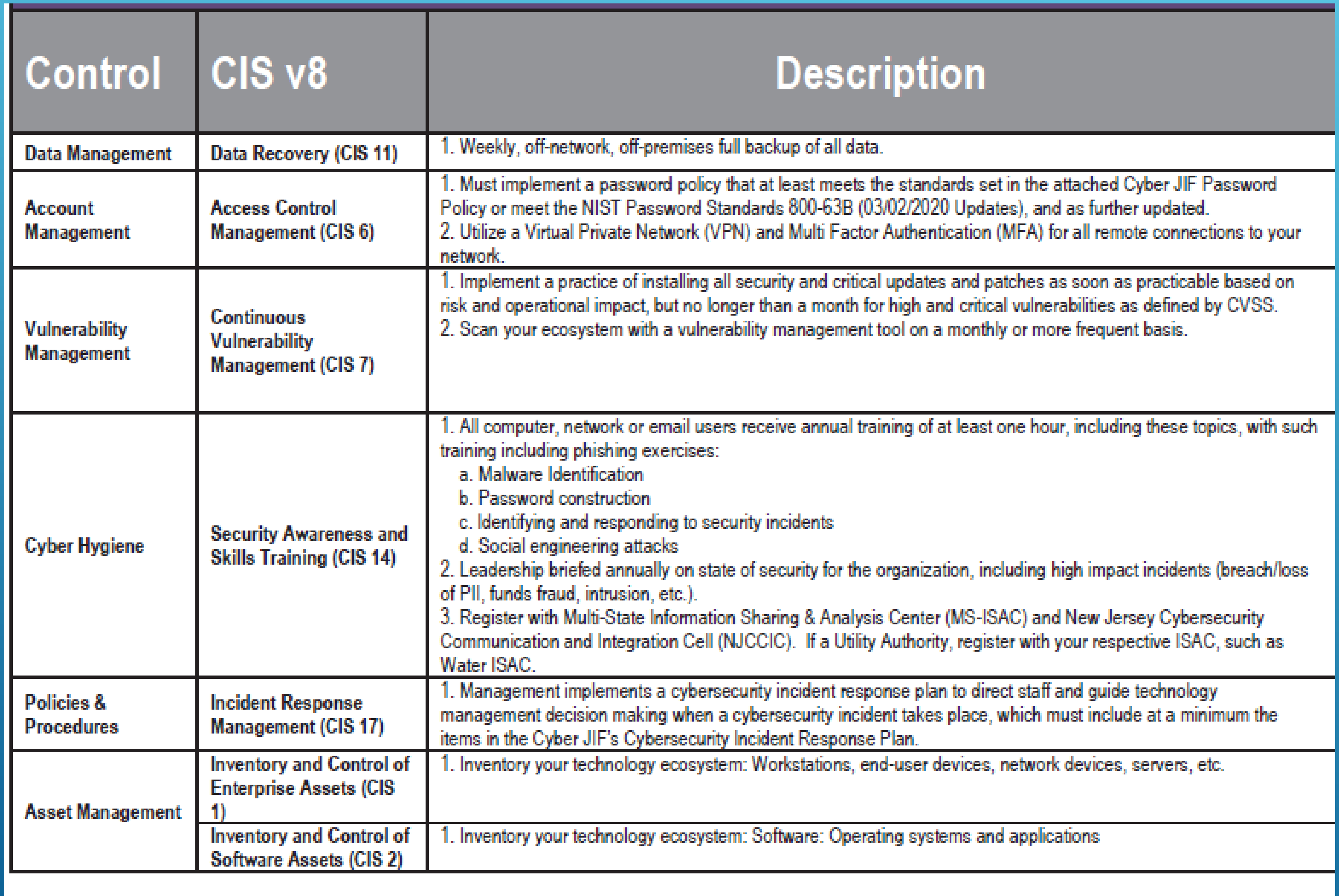
Getting Started!

1. GET A TECHNOLOGY EXPERT! STOP
2. Review the Cybersecurity Framework with your technology expert.
3. Develop a plan, timetable, and budget to implement the standards.
4. Once implemented, complete the Certification checklist.
5. Establish a process to annually review your technology risks and ensure the program continues to be met.

GMIS NEW JERSEY
An Association Of Government IT Leaders

- Even you have an in-house staff, use consultants and others to help
- Training is paramount!
- Communication is key!
  - Talk to your IT regularly!
- Review your JIF Cyber compliance requirements
  - Ensure you are in compliance
- Go Above the minimums

Basic Security

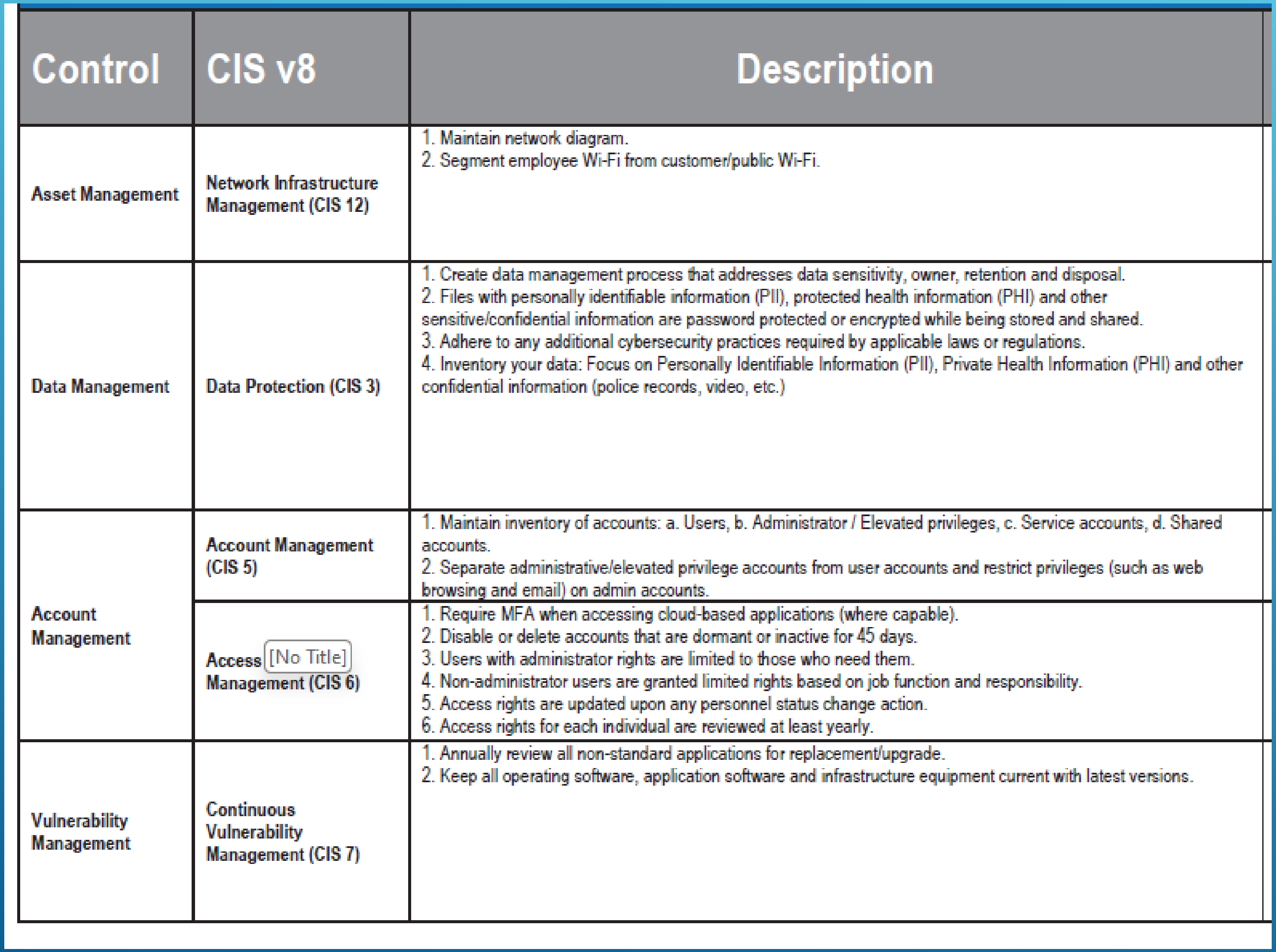


Control	CIS v8	Description
Data Management	Data Recovery (CIS 11)	1. Weekly, off-network, off-premises full backup of all data.
Account Management	Access Control Management (CIS 6)	1. Must implement a password policy that at least meets the standards set in the attached Cyber JIF Password Policy or meet the NIST Password Standards 800-63B (03/02/2020 Updates), and as further updated. 2. Utilize a Virtual Private Network (VPN) and Multi Factor Authentication (MFA) for all remote connections to your network.
Vulnerability Management	Continuous Vulnerability Management (CIS 7)	1. Implement a practice of installing all security and critical updates and patches as soon as practicable based on risk and operational impact, but no longer than a month for high and critical vulnerabilities as defined by CVSS. 2. Scan your ecosystem with a vulnerability management tool on a monthly or more frequent basis.
Cyber Hygiene	Security Awareness and Skills Training (CIS 14)	1. All computer, network or email users receive annual training of at least one hour, including these topics, with such training including phishing exercises: a. Malware Identification b. Password construction c. Identifying and responding to security incidents d. Social engineering attacks 2. Leadership briefed annually on state of security for the organization, including high impact incidents (breach/loss of PII, funds fraud, intrusion, etc.). 3. Register with Multi-State Information Sharing & Analysis Center (MS-ISAC) and New Jersey Cybersecurity Communication and Integration Cell (NJCCIC). If a Utility Authority, register with your respective ISAC, such as Water ISAC.
Policies & Procedures	Incident Response Management (CIS 17)	1. Management implements a cybersecurity incident response plan to direct staff and guide technology management decision making when a cybersecurity incident takes place, which must include at a minimum the items in the Cyber JIF's Cybersecurity Incident Response Plan.
Asset Management	Inventory and Control of Enterprise Assets (CIS 1)	1. Inventory your technology ecosystem: Workstations, end-user devices, network devices, servers, etc.
	Inventory and Control of Software Assets (CIS 2)	1. Inventory your technology ecosystem: Software: Operating systems and applications

GMIS NEW JERSEY
An Association Of Government IT Leaders

- Use all the free tools you can.
- Backups are a must
  - Both on premise and in the cloud!
- Computers and servers must be patched and updated regularly!
- Users must know the importance!
  - They are both your strength and weakness!

Intermediate Secuirty

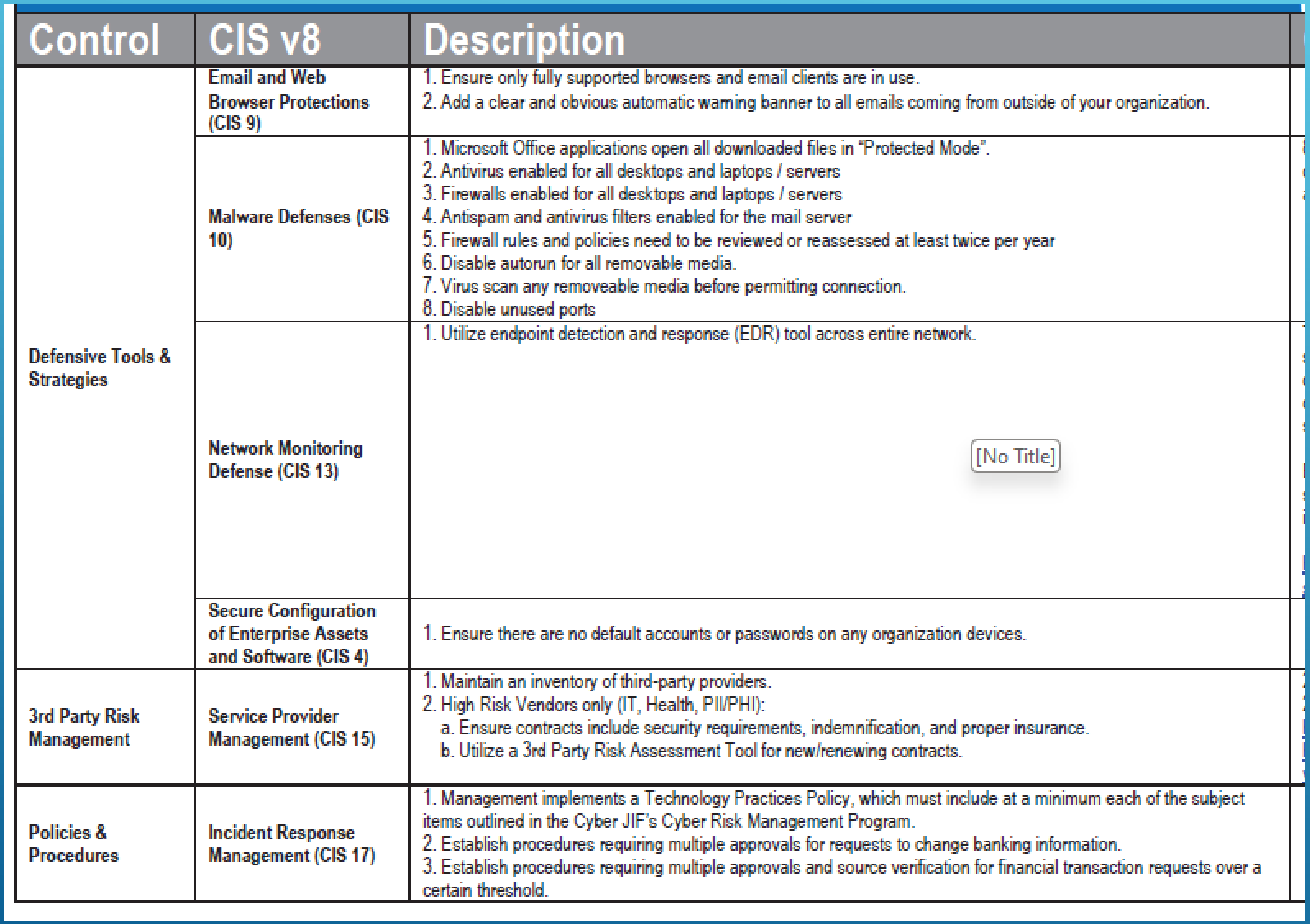


Control	CIS v8	Description
Asset Management	Network Infrastructure Management (CIS 12)	1. Maintain network diagram. 2. Segment employee Wi-Fi from customer/public Wi-Fi.
Data Management	Data Protection (CIS 3)	1. Create data management process that addresses data sensitivity, owner, retention and disposal. 2. Files with personally identifiable information (PII), protected health information (PHI) and other sensitive/confidential information are password protected or encrypted while being stored and shared. 3. Adhere to any additional cybersecurity practices required by applicable laws or regulations. 4. Inventory your data: Focus on Personally Identifiable Information (PII), Private Health Information (PHI) and other confidential information (police records, video, etc.)
Account Management	Account Management (CIS 5)	1. Maintain inventory of accounts: a. Users, b. Administrator / Elevated privileges, c. Service accounts, d. Shared accounts. 2. Separate administrative/elevated privilege accounts from user accounts and restrict privileges (such as web browsing and email) on admin accounts.
	Access [No Title] Management (CIS 6)	1. Require MFA when accessing cloud-based applications (where capable). 2. Disable or delete accounts that are dormant or inactive for 45 days. 3. Users with administrator rights are limited to those who need them. 4. Non-administrator users are granted limited rights based on job function and responsibility. 5. Access rights are updated upon any personnel status change action. 6. Access rights for each individual are reviewed at least yearly.
Vulnerability Management	Continuous Vulnerability Management (CIS 7)	1. Annually review all non-standard applications for replacement/upgrade. 2. Keep all operating software, application software and infrastructure equipment current with latest versions.

GMIS NEW JERSEY
An Association Of Government IT Leaders

- MFA is key!
  - Add MFA to all VPN and Server access.
  - Require MFA on all Cloud applications if possible
    - They can be a key weakness!
  - Wi-Fi should never be a part of your network
    - Make is a separate part!

Intermediate Security

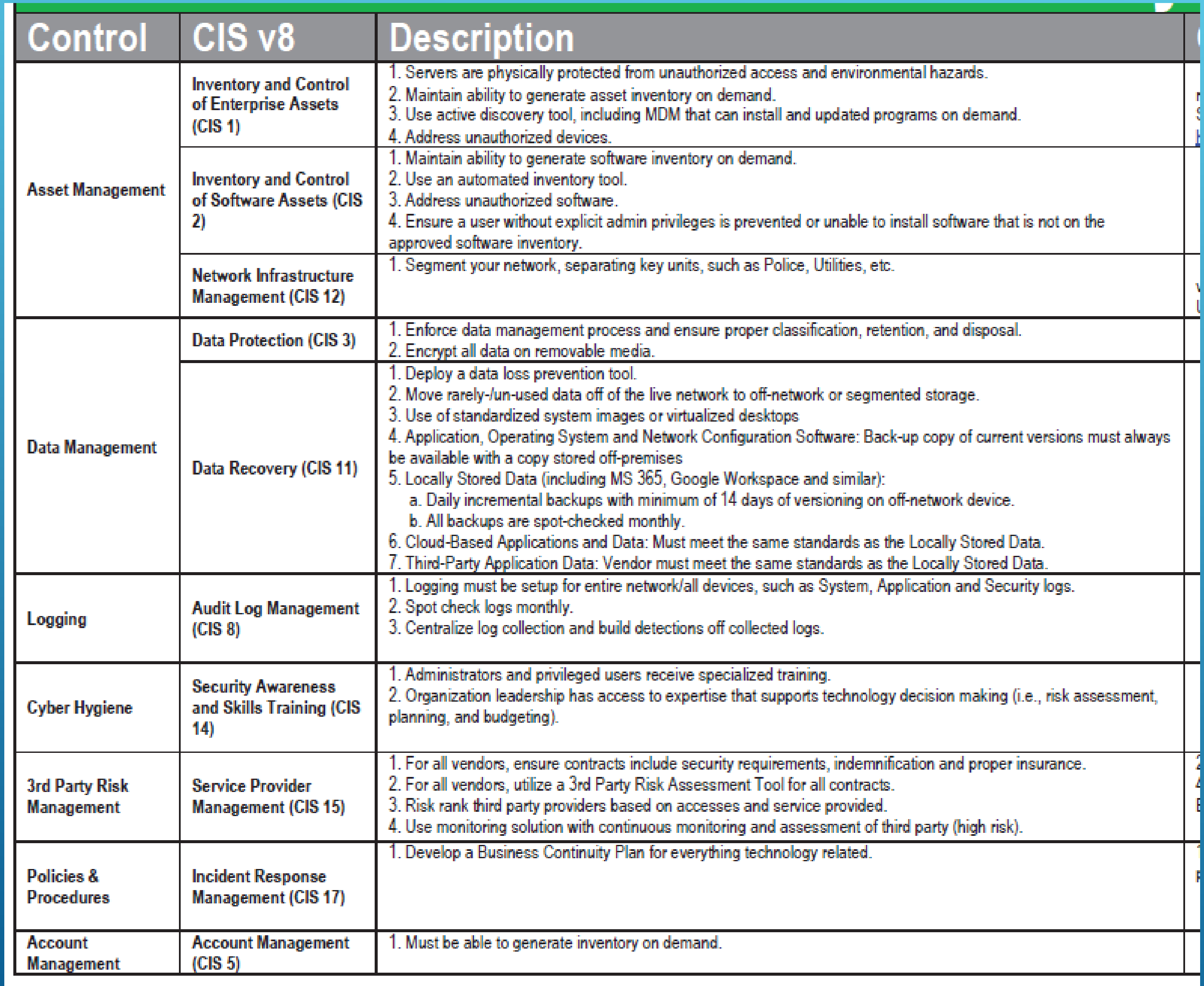


Control	CIS v8	Description
Defensive Tools & Strategies	Email and Web Browser Protections (CIS 9)	1. Ensure only fully supported browsers and email clients are in use. 2. Add a clear and obvious automatic warning banner to all emails coming from outside of your organization.
	Malware Defenses (CIS 10)	1. Microsoft Office applications open all downloaded files in "Protected Mode". 2. Antivirus enabled for all desktops and laptops / servers 3. Firewalls enabled for all desktops and laptops / servers 4. Antispam and antivirus filters enabled for the mail server 5. Firewall rules and policies need to be reviewed or reassessed at least twice per year 6. Disable autorun for all removable media. 7. Virus scan any removeable media before permitting connection. 8. Disable unused ports
	Network Monitoring Defense (CIS 13)	1. Utilize endpoint detection and response (EDR) tool across entire network. [No Title]
	Secure Configuration of Enterprise Assets and Software (CIS 4)	1. Ensure there are no default accounts or passwords on any organization devices.
3rd Party Risk Management	Service Provider Management (CIS 15)	1. Maintain an inventory of third-party providers. 2. High Risk Vendors only (IT, Health, PII/PHI): a. Ensure contracts include security requirements, indemnification, and proper insurance. b. Utilize a 3rd Party Risk Assessment Tool for new/renewing contracts.
Policies & Procedures	Incident Response Management (CIS 17)	1. Management implements a Technology Practices Policy, which must include at a minimum each of the subject items outlined in the Cyber JIF's Cyber Risk Management Program. 2. Establish procedures requiring multiple approvals for requests to change banking information. 3. Establish procedures requiring multiple approvals and source verification for financial transaction requests over a certain threshold.

GMIS NEW JERSEY
An Association Of Government IT Leaders

- Ensure AV and Malware solutions in place
- An MDR solution is a good tool.
  - Will be pricey but could save a small team!
- All 3rd party vendors need to be assessed.
  - Security Scorecard a must!
- Policies and procedures need to be updated and maintained.

Advanced Security

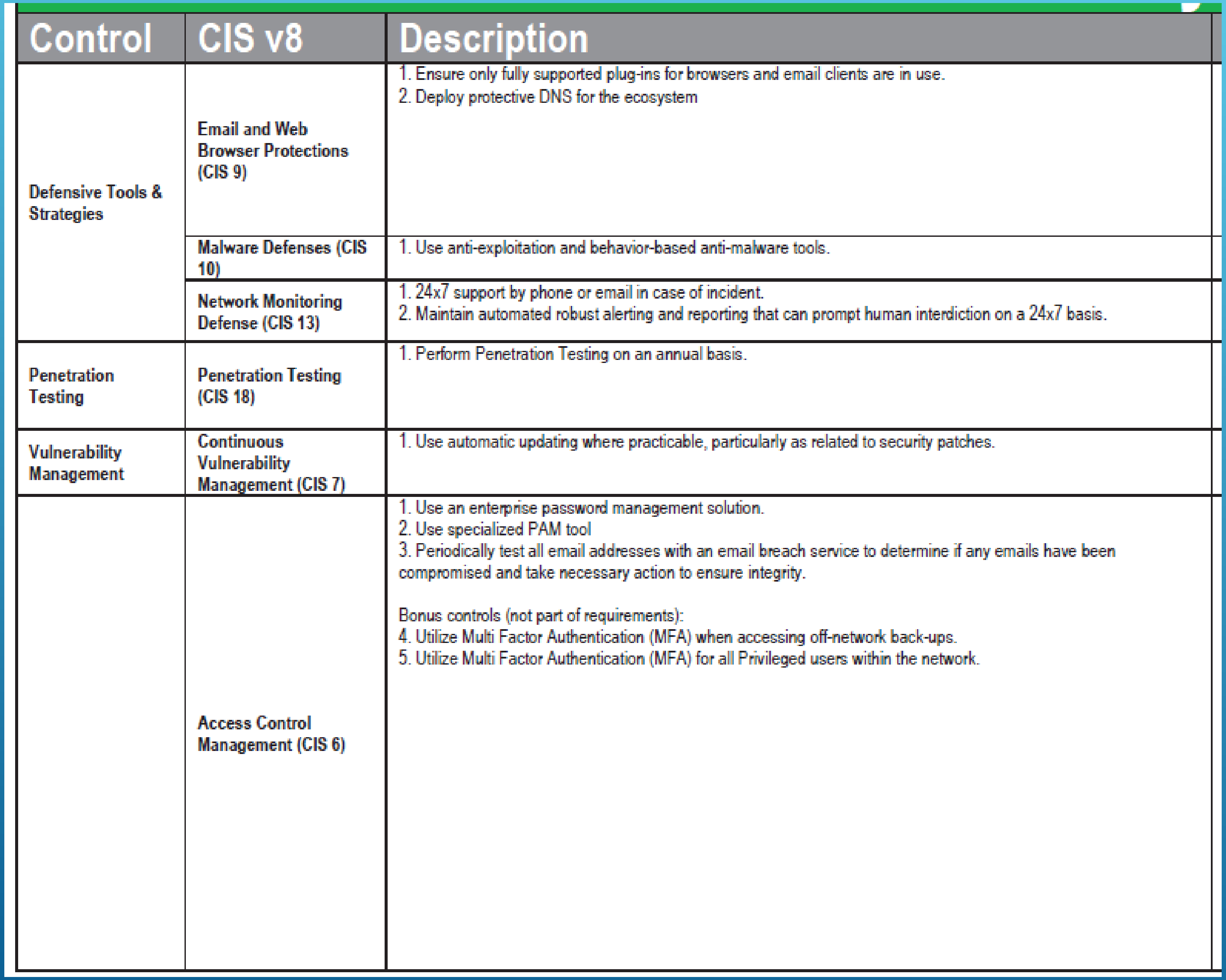


Control	CIS v8	Description
Asset Management	Inventory and Control of Enterprise Assets (CIS 1)	1. Servers are physically protected from unauthorized access and environmental hazards. 2. Maintain ability to generate asset inventory on demand. 3. Use active discovery tool, including MDM that can install and updated programs on demand. 4. Address unauthorized devices.
	Inventory and Control of Software Assets (CIS 2)	1. Maintain ability to generate software inventory on demand. 2. Use an automated inventory tool. 3. Address unauthorized software. 4. Ensure a user without explicit admin privileges is prevented or unable to install software that is not on the approved software inventory.
	Network Infrastructure Management (CIS 12)	1. Segment your network, separating key units, such as Police, Utilities, etc.
Data Management	Data Protection (CIS 3)	1. Enforce data management process and ensure proper classification, retention, and disposal. 2. Encrypt all data on removable media.
	Data Recovery (CIS 11)	1. Deploy a data loss prevention tool. 2. Move rarely-/un-used data off of the live network to off-network or segmented storage. 3. Use of standardized system images or virtualized desktops 4. Application, Operating System and Network Configuration Software: Back-up copy of current versions must always be available with a copy stored off-premises 5. Locally Stored Data (including MS 365, Google Workspace and similar): a. Daily incremental backups with minimum of 14 days of versioning on off-network device. b. All backups are spot-checked monthly. 6. Cloud-Based Applications and Data: Must meet the same standards as the Locally Stored Data. 7. Third-Party Application Data: Vendor must meet the same standards as the Locally Stored Data.
Logging	Audit Log Management (CIS 8)	1. Logging must be setup for entire network/all devices, such as System, Application and Security logs. 2. Spot check logs monthly. 3. Centralize log collection and build detections off collected logs.
Cyber Hygiene	Security Awareness and Skills Training (CIS 14)	1. Administrators and privileged users receive specialized training. 2. Organization leadership has access to expertise that supports technology decision making (i.e., risk assessment, planning, and budgeting).
3rd Party Risk Management	Service Provider Management (CIS 15)	1. For all vendors, ensure contracts include security requirements, indemnification and proper insurance. 2. For all vendors, utilize a 3rd Party Risk Assessment Tool for all contracts. 3. Risk rank third party providers based on accesses and service provided. 4. Use monitoring solution with continuous monitoring and assessment of third party (high risk).
Policies & Procedures	Incident Response Management (CIS 17)	1. Develop a Business Continuity Plan for everything technology related.
Account Management	Account Management (CIS 5)	1. Must be able to generate inventory on demand.

GMIS
NEW JERSEY
An Association Of Government IT Leaders

- Logging a key
  - Have a logging server!
- Password Management
  - Have a password manager
  - For both keys users and Admin
- Inventories
  - Know both HW and SW
- Data Recovery
  - Need to have a plan
  - Test it!
- JIF Cyber and Phishing Training

Advanced Security



Control	CIS v8	Description
Defensive Tools & Strategies	Email and Web Browser Protections (CIS 9)	1. Ensure only fully supported plug-ins for browsers and email clients are in use. 2. Deploy protective DNS for the ecosystem
	Malware Defenses (CIS 10)	1. Use anti-exploitation and behavior-based anti-malware tools.
	Network Monitoring Defense (CIS 13)	1. 24x7 support by phone or email in case of incident. 2. Maintain automated robust alerting and reporting that can prompt human interdiction on a 24x7 basis.
Penetration Testing	Penetration Testing (CIS 18)	1. Perform Penetration Testing on an annual basis.
Vulnerability Management	Continuous Vulnerability Management (CIS 7)	1. Use automatic updating where practicable, particularly as related to security patches.
	Access Control Management (CIS 6)	1. Use an enterprise password management solution. 2. Use specialized PAM tool 3. Periodically test all email addresses with an email breach service to determine if any emails have been compromised and take necessary action to ensure integrity. Bonus controls (not part of requirements): 4. Utilize Multi Factor Authentication (MFA) when accessing off-network back-ups. 5. Utilize Multi Factor Authentication (MFA) for all Privileged users within the network.

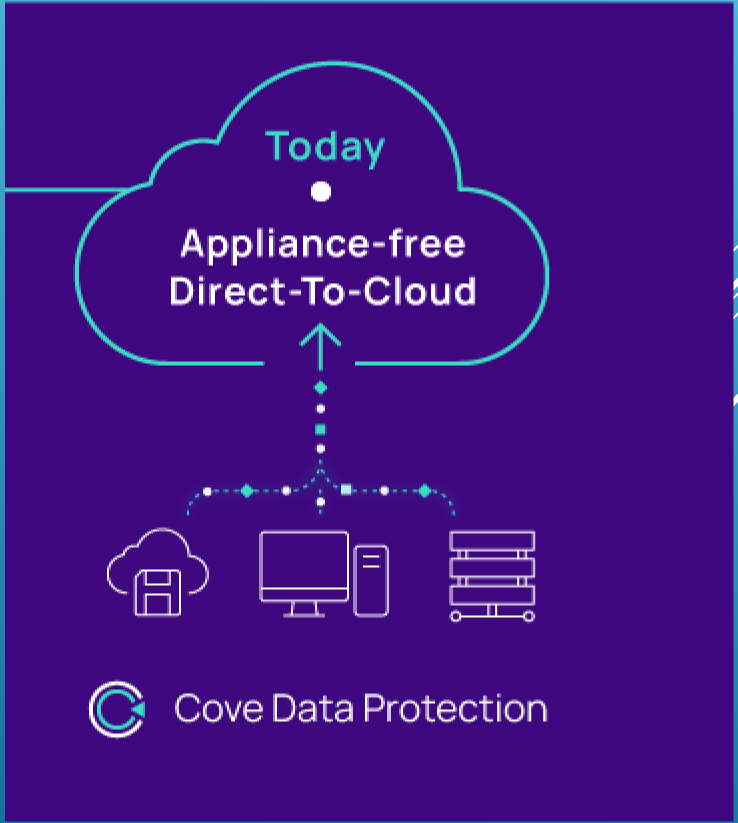
GMIS
NEW JERSEY
An Association Of Government IT Leaders

- Penetration Testing
  - Exterior is not enough
  - Test your inside too!
    - You will be surprised by what you see.
- Privileged Access Mgmt
  - Put a tool in place
- Backups
  - Look at local backups too for key personnel.
- Separate Key Networks
  - Police and City should not be touching!

Lessons Learned and Additions

GMIS NEW JERSEY
An Association Of Government IT Leaders

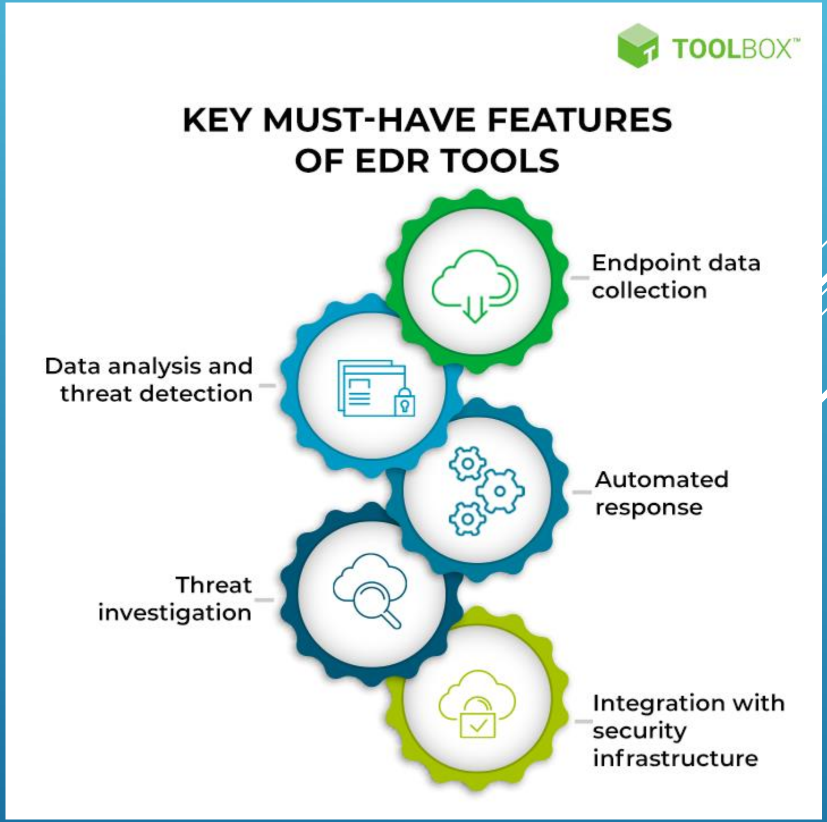
- MFA
  - Implement across network
  - Added MFA to server access
- Backups
  - Local Workstations not backed up
  - Key Personnel lost data
  - Added Cove Backup to key personnel
  - Test Backups
  - Ensure notifications set up for all backups
- Password Manager
  - Admin must have
  - Add for key personnel
- Network Monitoring
  - Ensure a simple yet solid solution in place
  - Something that notifies you of issues



Lessons Learned and Additions

GMIS
NEW JERSEY
An Association Of Government IT Leaders

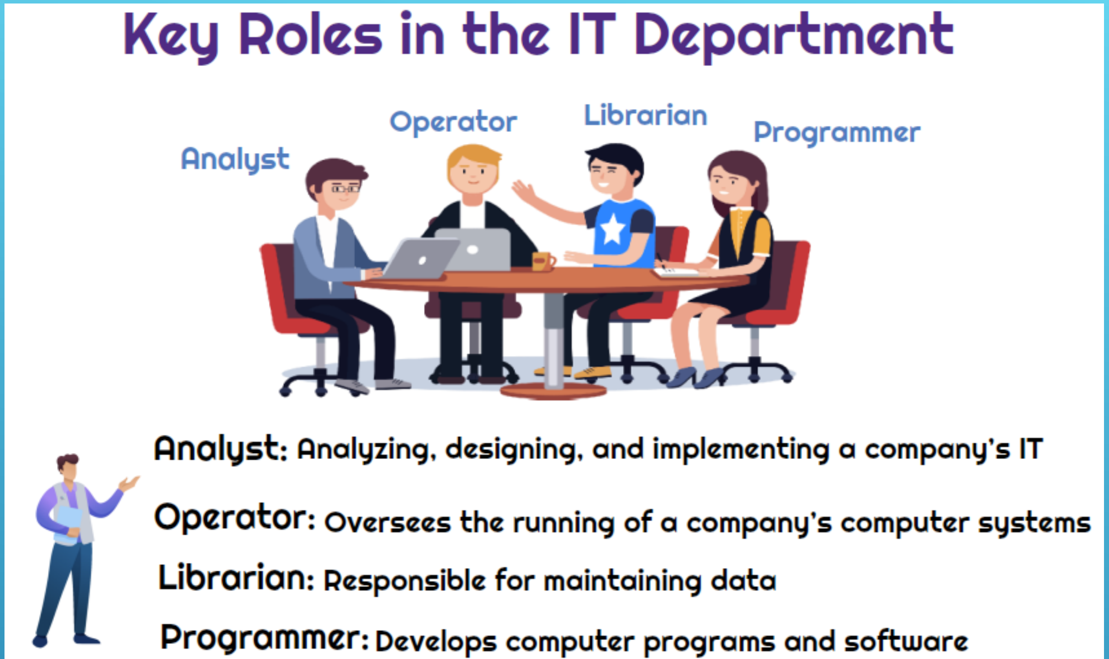
- AV and MDR
  - Put an MDR solution in place
    - A managed Disaster recovery
      - Someone 24/7 to review and monitor
  - If have a solid staff can do an EDR
    - Endpoint detection and response
- Firewalls
  - Make sure they are up to date
  - Make sure they have warranties and support in place
  - If possible, have a failover backup
- Network Segmentation
  - Separate key departments to protect
  - Police, Fire, DPW, Finance
- Laptops
  - Have remote work options in place



TOOLBOX™

KEY MUST-HAVE FEATURES OF EDR TOOLS

- Endpoint data collection
- Data analysis and threat detection
- Automated response
- Threat investigation
- Integration with security infrastructure



Key Roles in the IT Department

Analyst
Operator
Librarian
Programmer

Analyst: Analyzing, designing, and implementing a company's IT

Operator: Oversees the running of a company's computer systems

Librarian: Responsible for maintaining data

Programmer: Develops computer programs and software

We are all Partners!

Ransomware is not an IF anymore!
It is a WHEN!!
We need to work together to keep them out!

GMIS
NEW JERSEY
An Association Of Government IT Leaders

Resources

GMIS
NEW JERSEY
An Association Of Government IT Leaders

- GMIS
  - https://www.njgmis.org/
  - https://www.gmis.org/
- MS-ISAC
  - https://www.cisecurity.org/ms-isac
- NJCCIC
  - https://www.cyber.nj.gov/home-njccic
- CISA
  - https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools
- FBI
  - https://www.fbi.gov/investigate/cyber
- Have I Been Pwned
  - Email compromise tool
  - https://haveibeenpwned.com/
- JIF
  - Here is Atlantic County but find yours!
  - https://acmjif.org/